



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/853,708	05/14/2001	Takahiro Sugimoto	109460	6627
25944	7590	07/01/2005	EXAMINER	
OLIFF & BERRIDGE, PLC P.O. BOX 19928 ALEXANDRIA, VA 22320			HO, THOMAS M	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 07/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/853,708

Applicant(s)

SUGIMOTO, TAKAHIRO

Examiner

Thomas M. Ho

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 April 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-79 is/are pending in the application.
- 4a) Of the above claim(s) 25-36, 55, 56 and 68-72 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24, 37-54, 57-67 and 73-79 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 8/12/04, 5/14/01.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-79 are pending.

Restriction

2. Applicant's arguments regarding the restriction requirement are not persuasive.

The Examiner continues to hold that:

- Invention I has a separate utility such as a method for gathering information and using information for the purpose of developing a security policy or set of commands such as the building of a firewall in a network.
- Invention II has a separate utility as being a device or method which allows one to readjust the policy such as a program to allow network settings to be configured, such as bots or programs which regulate total throughput.
- Invention III has a separate utility as being a device or method which can assess the current state of security such as network auditing tools which scan a firewall for vulnerabilities. One of these tools is particularly well known in the art and is known as the "The System Administrator Tool for Analyzing Networks" (SATAN).
- Invention IV has separate utility as a report generator based on collection of data using analyzed data such as Microsoft Excel or the VB Crystal Reports.

Art Unit: 2134

These inventions are distinct for the reasons given above and while related to the field of computer security, embody independent inventions within that field and would consequently require different searches in their different subclasses.

Therefore, the Examiner maintains the requirement for restriction. Claims 1-24, 37-54, 57-67, 73-79 from Group I have been elected. All other claims have been removed from consideration.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1-24, 37-54, 57-67, 73-79 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

MPEP 2105 states

"The laws of nature, physical phenomena and abstract ideas" are not patentable subject matter.

Art Unit: 2134

The Examiner contends that Applicant's invention is an abstract idea. A security policy in itself, even if established (see below) is neither a process, machine, manufacture, or composition of matter but is a common idea or concept shared among members of an organization.

The Examiner further holds Claims 1-24, 37-54, 57-67, 73-79 to be non-statutory because it does not produce a concrete, useful, or tangible result. (all three requirements are necessary)

"For such subject matter to be statutory, the claimed process must be limited to a practical application of the abstract idea or mathematical algorithm in the technological arts. See Alappat, 33 F.3d at 1543, 31 USPQ2d at 1556-57 (quoting Diamond v. Diehr, 450 U.S. at 192, 209 USPQ at 10). See also Alappat 33 F.3d at 1569, 31 USPQ2d at 1578-79 (Newman, J., concurring) ("unpatentability of the principle does not defeat patentability of its practical applications") (citing O'Reilly v. Morse, 56 U.S. (15 How.) at 114-19). A claim is limited to a practical application when the method, as claimed, produces a concrete, tangible and useful result; i.e., the method recites a step or act of producing something that is concrete, tangible and useful. See AT &T, 172 F.3d at 1358, 50 USPQ2d at 1452." MPEP 2106 B(2)b(ii)

"The claimed invention as a whole must produce a "useful, concrete and tangible" result to have a practical application." MPEP 2601 Section II A

"A process that consists solely of the manipulation of an abstract idea is not concrete or tangible. See In re Warmerdam, 33 F.3d 1354, 1360, 31 USPQ2d 1754, 1759 (Fed.

Cir. 1994). See also Schrader, 22 F.3d at 295, 30 USPQ2d at 1459.” MPEP 2601 Section II A

“A process that merely manipulates an abstract idea or performs a purely mathematical algorithm is nonstatutory despite the fact that it might inherently have some usefulness. In Sarkar, 588 F.2d at 1335, 200 USPQ at 139” MPEP 2106 B(2)b(ii)

Claims 1-24, 37-54, 57-67, 73-79 are further rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility.

Claim 1 recites “a method of establishing a security policy for a predetermined organization”

However, the Examiner contends that no security policy has actually been established by claim

1. At best, *a security policy draft has been adjusted* on the basis of particular differences. The mere adjustment of the draft however is not tantamount to establishing the actual security policy. For this reason, the Examiner holds that the method recited is inoperative.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1-24, 37-54, 57-67, 73-79 rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. Details or methods of analysis critical or essential to the practice of the invention, but not included in the claim(s) is not enabled by the disclosure. See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976). Applicant's claims are a method of establishing a security policy for a predetermined organization using the steps of draft preparation, analysis, and adjustment. The Examiner holds that such steps are deficient in that one of ordinary skill in the art would not be able to establish the security policy based on this disclosure. The establishment of a security policy would require significant manipulations, organization, and description of how it would be implemented with the particular entities of an organization. These details are essential and cannot simply be glossed over.

Furthermore, steps depicting the method of analysis must also be given. Without any further steps delimiting the analysis step of examining differences between the security policy draft and the realities of the organization, the realization of the steps in the claim would be wholly dependent on the individual merit and skill of the individual artisan.

Furthermore, the Examiner maintains it is nontrivial to prepare a security policy draft, yet no steps for the creation of the draft preparation step is provided. A security policy draft is a substantial scaffolding of the actual security policy itself. Without any details given the Examiner would maintain that such a method is tantamount to a method of designing a system (eg. A rocket) by

A) designing the first half

Art Unit: 2134

B) designing the second.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1-24, 37-54, 57-67, 73-79 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Information Security Policies and Procedures: A practitioner's Guide" by Thomas Peltier, published in 1998.

- As per claim 1, Peltier teaches a method of establishing a security policy for a predetermined organization, the method comprising: a draft preparation step of preparing a security policy draft (1: A good writer should be able to create an initial draft of a policy", page 41, paragraph 10.3. - Write the Initial Draft and Prepare Illustrations);
- an analysis step of examining a difference between the security policy draft and realities of the organization ("Have you noted a variation from the policy of some other significant security vulnerability? Has it been resolved? If not, is satisfactory progress toward resolution been made?", page 253, 6.2 - Information Security Standards);
- an adjustment step of adjusting the security policy draft on the basis of the difference of adjusting operation rules of an actual information system belonging to the organization

on the basis of the difference ("16. Review and reconcile comments from the Critique Panel. 17. Prepare second draft based on critiques", page 45).

- Peltier does not explicitly teach an analysis but teaches the answering of a series of questions, through which an analysis occurs in order to answer the posed questions.

Analysis is inherent in the gathering of data through asking questions and formulating an answer to said questions.

As per claims 2, 11, 19, 57-61, 67, 73-76, 79 Peltier teaches the method and apparatus of establishing a security policy according to claim 1, wherein the draft preparation step comprises:

- a drafting or establishing step of preparing a security policy draft on the basis of the answers ("once the research and reading is finished, the interviews are complete, and the physical layout of the document has been determined, it will be necessary to begin to write the policies, standards and procedures", page 41, paragraph 10.3 Write the Initial Draft and Prepare Illustrations).
- a preparation step of preparing inquiries to be submitted to members of an organization and an inquiry step of submitting the prepared inquiries to the members and an answer acquisition step of acquiring from the members answers to the inquiries ("it will be necessary to interview senior management, department heads, first line supervisors, and users", page 41, paragraph 10.2 - Conducting Interviews). While preparing questions is not specifically taught, Peltier does teach questions, submitting questions, and acquiring answers as the essential nature of an interview, since it would not be possible to conduct an interview without asking and answering questions. Since questions are taught, the

questions must obviously be prepared and therefore the preparation of questions is inherent in the existence and the asking of the questions. Similarly, the interview process consists of asking questions and getting the answers to the questions. Storing the answers to the questions would be a natural part of the interview process and would be useful so that the interviewer could retrieve the answers to the questions at a later date in order to know what answers were given to the questions. Therefore, storing the answers to questions is inherent in the interview process.

As per claim 4, 13, 21, 62-64 Peltier teaches the method of establishing a security policy according to claim 2, wherein the answer acquisition step includes at least one of the steps of:

- integrating the answers acquired from a single member from among the acquired answers and storing the integrated answers into storage means as answers of a single member to be inquired ("the second or updated round should include as many of the recommendations from the support team as possible. It is the responsibility of the core group to review every suggestion, and to either implement the suggestion or meet with the group member and explain why no action is being taken", page 141, paragraph 1);
- re-submitting inquiries to members if contradictory answers are included in the answers, to thereby resolve contradiction, and storing the answers into the storage means after all the comments and suggestions have been reviewed and the draft has been updated, send the document out for a second round of review. Try and indicate where the updated draft; document is different from the original", page 141, paragraph 2);

- assigning weights to answers according to job specifications of the members to be inquired if contradictory answers are included in the answers, to thereby determine answers and store the answers into the storage means ("There is a weighting system for comments. All comments are equal some are more equal than others - know who is suggesting what", page 142, paragraph 4 - comment key points), wherein comments are weighted with respect to the member who made the comment, and a member's job skills and job specifications are inherent in who the member is, as that subject matter expertise in the job is the basis for the authority a member conveys in his respective field. The member's opinion carries more weight if the issue on which the opinion is being expressed is an area in which said member works at a job, and an opinion on an issue in which the member does not have a job, knowledge or expertise would carry less weight than another member who has a job in that area. Therefore a weighting that gives more weight to an opinion based on who is suggesting the opinion inherently includes that member's job which is the basis from which the authority to make a suggestion or voice an opinion is derived.

As per claims 5, Peltier teaches the method of establishing a security policy according to claim 2, wherein the analysis step comprises at least one of:

- a contradiction inspection step of inspecting whether or not contradictory answers are included in the answers, ("some comments may require a meeting of the groups to iron out any major differences. It is best to resolve the conflict before the document is

published", page 141, paragraph 3), wherein contradiction answers between two or more people are inherent as the result of the major differences and conflict of opinions between two or more individuals taught by the reference;

- a first difference detection step of inspecting a difference between an information system virtually desired on the basis of the answers and the security policy, by means of comparison ("Review and reconcile comments from the critique panel. 17 Prepare second draft based on critiques. 20. Prepare a final draft based on", page 45), wherein the first draft and second drafts are the security policy and the final draft is the virtually desired security policy;
- a second difference detection step of verifying the virtually- desired information system by means of examination of a real information system and inspecting a difference between the verified information system and the security policy draft by means of comparison ("have you noted a variation from the policy of some other significant security vulnerability? Has it been Resolved? If not, is satisfactory progress toward resolution been made?"), page 253, 6.2 - Information Security Standards), wherein the step of inspection is inherent in answering the questions because without an inspection, the person answering the questions would not be able to answer the questions regarding the state of the real security system. While output is not specifically taught by the Peltier reference, the creation of a new draft of the security plan by incorporating answers to the questions is taught, and presentation of the next and final drafts of the security plan is also taught. Since a proposal or security plan must be output in some way before it is

presented, either on paper or in electronic display form, output is inherent in the creation of a draft and in the presentation of a draft.

As per claim 7, Peltier teaches the method of establishing a security policy, further comprising a diagnosis step of diagnosing the security state of the organization, wherein a result of diagnosis performed in the diagnosis step is submitted to the organization, where in the organization can become conscious of a necessity for a security policy ("Identifying threats; identifying vulnerabilities; identifying loss impact", Page 136, paragraph 5), wherein threats, vulnerabilities and loss impact constitute a security diagnosis.

As per claims 14 and 22, Peltier teaches the method of establishing a security policy, wherein the establishment step involves establishment of three types of security policies: namely, an executive- level security policy which describes the organization's concept and policy concerning information security, in conformity with global guidelines ("an organizational information security coordinator is appointed by organization management to develop, implement, and maintain an organizational IS program consistent with corporate and organizational objectives", page 212, paragraph 4.2.1. - Organizational Coordinators; a corporate-level security policy which describes an information security system embodying the executive-level security policy ("this individual is responsible for maintenance of the program's vision, goals, and elements, and for proposing necessary changes to the IS Steering Committee for approval"; page 212, paragraph 3.2. - Corporate Information Security Coordinator); a product-level security policy which describes measures to implement the executive-level security policy with reference to the

Art Unit: 2134

corporate-level security policy ("these are the business unit management charged with the responsibility to provide appropriate security of the organization's information assets including management, operation and technical controls that support the overall policy directives and standards", page 44, paragraph 13.2 - Application, System, and Information Functional Owners), wherein the software applications are the individual products that are used by the organization. Microsoft Windows would be an example of an application.

As per claims 15 and 23, Peltier teaches the method of establishing a security policy, wherein the corporate-level security policy includes two types of corporate-level security policies namely, a top-level security policy describing standards for the information security system of the overall organization ("program-level and topic-specific policies both address policy on a broad level; they usually encompass the entire enterprise", page 55, paragraph 8.3. - Application specific policy), such as ("Thesis Statement, Relevance, Responsibility, Compliance", page 55, paragraph 8.2 - Topic-specific policy; a sub-level security policy describing standards for individual units constituting the information security system of the organization ("the application specific policy focuses on one specific system or application", page 55, paragraph 8.3. - Application specific policy), such as ("Who has the authority to read or modify data? Under what circumstances can data be read or modified?", page 55, paragraph 8.3. - Application specific policy), wherein the application and person specific aspects of security are sub-level.

Art Unit: 2134

As per claims 16 and 24, Peltier teaches the method of establishing a security policy, wherein the product-level security policy includes two types of product-level policies; namely, a first-level security policy described in natural language ("it will be necessary to establish the standards for account passwords", page 131))

a second-level security policy describing settings of individual devices constituting the information security system ("it will be necessary to establish the standards for account passwords. Included in this will be the following subjects: using alphanumeric characters; proper password length five to eight characters; choosing passwords that are not inherently weak", page 131), wherein the first level state the policy that there will be established standards for passwords and the second level gives the specific settings or standards for passwords.

As per claim 17, Peltier teaches the method of establishing a security policy, further comprising an analysis step of:

- examining a difference between the security policy draft and realities of the organization with the analysis step further comprising at least one of a contradiction inspection step of inspecting whether or not contradictory answers are included in the answers; ("have you noted a variation from the policy of some other significant security vulnerability? Has it been Resolved? If not, is satisfactory progress toward resolution been made?", page 253, 6.2 – Information Security Standards);
- a first difference detection step of inspecting a difference between the security policy and an information system virtually designed on the basis of the answers, by means of comparison; ("16. Review and reconcile comments from the critique panel. 17 Prepare

second draft based on critiques. 20. Prepare a final draft based on", page 45), wherein the first (1r0 and second draft are the security policy and the final draft is the virtually designed security policy;

- a second difference detection step of verifying the virtually- desired information system by means of examination of a real information system and inspecting a difference between the verified information system and the security policy draft, by means of comparison, ("have you noted a variation from the policy of some other significant security vulnerability? Has it been Resolved? If not, is satisfactory progress toward resolution been made?", page 253, 6.2 - Information Security Standards), wherein the step of inspection is inherent in answering the questions because without an inspection, the person answering the questions would not be able to answer the questions regarding the state of the real security system.

As per claims 37, Peltier teaches the analyzer for analyzing a difference between a security policy and an information system of an organization, further comprising: matching means for matching the answers by means of elimination of contradiction on the basis of the information about contradiction, thus producing answers free of contradiction ("some comments may require a meeting of the group to iron out any major differences" page 141, paragraph 3); establishment means for virtually establishing an information system for the organization on the basis of the answers produced by the matching means (Eç16. Review and reconcile comments from the critique panel. 17. Prepare second draft based on critiques", page

Art Unit: 2134

45); and difference output means for outputting a difference between the configuration of the virtually-established information system and a security policy, by means of comparison ("20. Prepare final draft based on critiques", pages 44 - 45), where the differences between the first draft designed system and the eventual policy are incorporated into the later and eventual final draft of the policy. While Peltier does not specifically use the word contradiction, he does teach a meeting for dealing with parties that have differences between them, where contradictions or contradictory positions are inherent in differences of opinion between two or more parties.

Claims 3, 12, 20, are rejected under 35 U.S.C. 103(a) as being unpatentable over the book "Information Policy and Procedures: A Practitioner's Guide" by Thomas Peltier, published in 1998 in view of the book ("Computer Security" by Norman Enger), published in 1980.

As per claims 3, 12, 20, Peltier teaches a method of establishing a security- policy wherein the preparation step involves preparation of inquiries. However, Peltier does not teach a method based on the job specifications of members to be inquired.

Enger does teach a method of preparing questions based on a specific job ("some of the questions that should be documented for the DBA", page 235-236), wherein a Data Base Administrator is a specific job associated with computer security. Both inventions are analogous art because they both involve survey questions directed at asking security team members questions about computer security.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to make the survey questions specific to a particular job because that person would

Art Unit: 2134

know the specific aspects of their job and thus the security issues surrounding that area. It would be obvious to take advantage of the person's subject matter expertise in a job in order to enhance security in that area, and the most obvious way to probe that expert's knowledge would be to ask questions that are specifically oriented toward that person's job.

Claims 6, 8, 10, 18, are rejected under 35 U.S.C. 103(a) as being unpatentable over the book "Information Policy and Procedures: A Practitioner's Guide" by Thomas Peltier, published in 1998.

As per claims 6 and 18, Peltier teaches the method of establishing a security policy. Peltier does not teach a measurement step of devising measures addressing the inspected difference in conjunction with the priority of the measures. However, Peltier does teach a scoring measure in the form of information identification ("priority: medium, 'high" and "criticality: critical, not critical", page 250) and scoring in terms of scoring controls ("loss impact'. low, medium, high", page 252). Official Notice is taken that a scoring measure either to rank them or to give a rating is old and very well known in the art of evaluating. It would be very obvious to score the above listed items in order to identify which of the said items is in need of the most effort to affect improvement and to indicate which items are the closest to conforming with standards and thus do not need effort applied to affect improvement. This would be useful in order to determine where to allocate time, money, people and other limited corporate resources so that optimal use is made of these resources.

Art Unit: 2134

As per claim 8, Peltier teaches a method of establishing a security policy, further comprising a priority planning step of planning, in sequence of priority, implementation of the security measures which have been devised with priority (page 236 – 237, paragraph 4.1 Program Implementation Plan), thereby embodying a budget of the organization ("Information security costs will primarily be Operations and Maintenance budget items, along with some Capital Budget Items", page 227 - 228).

As per claim 10, teaches the method of establishing a security policy according to claim 8, further comprising a security enhancement measures implementation step of implementing the security measures in accordance with the plan (page 236, paragraph 4.1. – Program implementation Phase).

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over the book ("Information Policy and Procedures: A Practitioner's Guide" by Thomas Peltier, published in 1998 in view of Bowman-Amuah (US 6,324,647).

As per claim 9, Peltier teaches the method of establishing a security policy wherein the security measures comprise:

introduction ("Awareness activities tell the audience what you want them to do, and why they should do it. Before you can do that, however, you need to tell them what the program elements are, and why they are being implemented", page 236, paragraph 3) and testing "performing periodic reviews of access and control requirements to ensure that information access and control

Art Unit: 2134

requirements remain appropriate and are function adequately", page 184, bullet 6), wherein ensuring that something is functioning adequately is a test;

training for compelling employees to respect a security policy CW. Determine training requirements, C. Develop training plan; D. Manage training activities", page 26, item 11. -

Training; auditing operations on the basis of the security policy, ("effectiveness monitoring or compliance monitoring must be continuous in order to provide feedback on the program. Again, two areas should be monitored for effectiveness: the information Security program and the IS controls that have been implemented", page 243, paragraph 5.4.4 - Maintaining Program Effectiveness Monitoring), where auditing is by definition compliance monitoring; reviewing the security policy, to establish a calendar to review policies, standards, and procedures on a regular basis", page 45, step 25),.

Peltier does not teach analysis of security logs or monitoring a network. Bowman- Amuah does teach analysis of system logs, ("analyzing security logs", column 140, line 17) and monitoring of a network, ("detecting unauthorized attempts to access a network" column 140, 5 lines 1), where monitoring is inherent in detecting because something must be monitored before something can be detected. Both are analogous are because both inventions are concerned with developing and maintaining security policies.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the security policy aspects of the Peltier with the network administration elements of the Bowman-Amuah invention in order to develop an invention that takes practical real-time data input from the network system and uses it to identify where there are security problems in order

Art Unit: 2134

to insure that said problems are addressed in the next revision of a security policy. This would provide a real time assessment of security problems that would point to areas having the most real time problems and would be a more efficient means for gathering information than use of surveys or interviews because the data would be transmitted from an active computer network and would provide supporting evidence that a problem exists. This type of data would be less subjective to opinion than surveys or interviews and would also be less costly and less time consuming to collect.

Conclusion

10. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist Telephone: 571-272-2100 Fax: 703-872-9306

Customer Service Representative Telephone: 571-272-2100 Fax: 703-872-9306

TMH


David Y. Jung
Primary Examiner

6/25/08

Art Unit: 2134

June 26th, 2005

David Y. Jung
Primary Examiner
Primary Examiner


6/26/06